UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,806	03/15/2004	Jeffrey A. Von Arx	115.0080US01	1609

62058 7590 11/24/2009

PAULY, DEVRIES SMITH & DEFFNER, L.L.C.
PLAZA VII- SUITE 3000
45 SOUTH SEVENTH STREET
MINNEAPOLIS, MN 55402-1630

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
11/24/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/800,806	VON ARX ET AL.	
	Examiner	Art Unit	
	BENJAMIN A. KAPLAN	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 August 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,13-15,27,29,59,61,65 and 68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,13-15,27,29,59,61,65 and 68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the most recent papers filed on August 4, 2009.

Response to Arguments and Amendments

2. The rejection of claims 30-39, 46-49 and 56-58 under 35 USC § 101 is withdrawn as being moot in view of their cancellation.

3. Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 3, 13-15, 27, 29, 59, 61, 65 & 68 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent Application Publication No. US 2004/0260363 A1 (Arx et al.).

As Per Claim 1: Arx et al. teaches: **An apparatus for securely authenticating a data exchange session with an implantable medical device, comprising:**

- an external device comprising a key generator configured to dynamically generate a crypto key for each data exchange session with an implantable medical device;

(Arx et al., Paragraph [0043], Lines 20-26, "In another embodiment, both implantable and external devices are capable of randomly generating new public/private key pairs by the RSA algorithm or through some other standard key pair generating algorithm. In this embodiment, new keys can be generated when the physician commands it via secure short-range inductive telemetry.").

An external device randomly generating key pairs is dynamically creating keys.

-the external device configured to establish an inductive telemetric link to the implantable medical device and to download the crypto key to the implantable medical device through the inductive telemetric link;
- the external device configured to then transact the data exchange session with the implantable medical device through a long range telemetric link authenticated with the crypto key

(Arx et al., Claim 1, "A method for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

implementing a telemetry interlock which limits any communications between the ED and the IMD over the telemetry channel;

releasing the telemetry interlock by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD;

authenticating the IMD to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD;

authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED; and,

allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD and ED have been authenticated to one other.").

With the external device generating key pairs as seen above in the cited portion of paragraph 43 it is handled through a short-range inductive telemetry. With a interlock released via a short-range communications channel the implantable medical device (IMD) and an external device (ED) authenticate each other by use of the generated keys.

As Per Claim 3: The rejection of claim 1 is incorporated and further Arx et al. teaches:

- an authentication component configured to employ the crypto key during the data exchange session, comprising at least one of:

- a command authenticator to authenticate commands exchanged through the external device with the implantable medical device and

- a data integrity checker configured to check the integrity of the data received by and transmitted from the external device

- a data encrypter configured to encrypt the data received by and transmitted from the external device

(Arx et al., Paragraph [0019], "Authentication refers to the mechanisms or protocols by which the participants in a communications session may reliably identify one another. An authentication protocol may be implemented using either secret key or public key cryptography to allow an implantable medical device (IMD) and an external device (ED) to authenticate one another. A data communications session between the IMD and ED over the telemetry channel is allowed to occur only after the IMD and ED have been authenticated to one other. With authentication by either public key or secret key cryptography, the IMD is authenticated to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD, and the ED is authenticated to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED.").

As Per Claim 13: The rejection of claim 1 is incorporated and further Arx et al. teaches:

- the external device comprises a programmer

(Arx et al., Paragraph [0002], "Implantable medical devices (IMDs), including cardiac rhythm management devices such as pacemakers and implantable cardioverter/defibrillators, typically have the capability to communicate data with an external device called an external programmer via a radio-frequency telemetry link. One use of such an external programmer is to program the operating parameters of an implanted medical device. For example, the pacing mode and other operating characteristics of a pacemaker are typically modified after implantation in this manner. Modern implantable devices also include the capability for bidirectional communication so that information can be transmitted to the programmer from the implanted device. Among the data that may typically be telemetered from an implantable device are various operating parameters and physiological data, the latter either collected in real-time or stored from previous monitoring operations.").

As Per Claim 14: The rejection of claim 13 is incorporated and further Arx et al. teaches:

- the crypto key is provided from the programmer to a repeater

(Arx et al., Paragraph [0043], "With either public key or secret key authentication, it is evidence of possession of a particular key which authenticates a device. In general, all authentication protocols are only as secure as the private keys in the case of public key cryptography and the secret keys in the case of secret key cryptography. For this reason the private or secret keys should be long (e.g., 128 bit in one embodiment). For

added security, the private or secret key may be either hardwired into a device at the factory or generated internally by the device, and then prevented from being read out by telemetry. For example, a private key may be programmed into a device during manufacture, with its corresponding public key then included with the product documentation or obtainable through short-range inductive telemetry. A physician can then program the device's public key into a home monitor, a portable repeater, or a programmer. All external devices have unique public and private authentication keys as well, with the public key included with the product documentation. A physician can thus program a number of external device's public keys into an implantable device. In another embodiment, both implantable and external devices are capable of randomly generating new public/private key pairs by the RSA algorithm or through some other standard key pair generating algorithm. In this embodiment, new keys can be generated when the physician commands it via secure short-range inductive telemetry.").

As Per Claim 15: The rejection of claim 1 is incorporated and further Arx et al. teaches:

- the external device comprises a patient designator

(Arx et al., Paragraph [0028], "Once authentication and release of the telemetry interlock have occurred, the IMD and the ED can proceed to communicate data over the long-range telemetry link with each device knowing that the other is not an impostor. If the data is sent in the clear during the data communications session, however, an eavesdropper could intercept the data and compromise the patient's privacy. It may

therefore be desirable to encrypt some or all communications between the ED and the IMD during the data communications session. As stated earlier, secret key encryption is much less computationally intensive than public key encryption and is preferred for transmitting relatively large amounts of data. If secret key cryptography is used for authentication, the ED and IMD can use the same secret key for data transmission. If public key cryptography is used for authentication, secret key cryptography can be used for data communications, where one of either the ED or the IMD transmits to the other of either the ED or the IMD a secret session key encrypted by the latter's public key. That secret session key can then be used by both participants to encrypt data.").

As Per Claim 27: The rejection of claim 1 is incorporated and further Arx et al. teaches:

- the crypto key comprises at least one of a 128-bit crypto key and a symmetric crypto key

(Arx et al., Paragraph [0013], "The encryption and decryption keys may be the same or different depending upon the type of cryptographic algorithm which is used. In secret key cryptography, both participants in a communication share a single secret key which is used for both encryption and decryption of a message. Thus a message m encrypted by a secret key encryption function E with a key k is recovered by applying the decryption function D with same key k:").

As Per Claim 29: The rejection of claim 1 is incorporated and further Arx et al. teaches:

- the implantable medical device comprises at least one of an implantable cardiac device, neural stimulation device, and drug therapy dispensing device

(Arx et al., Paragraph [0001], "This invention pertains to implantable medical devices such as cardiac pacemakers and implantable cardioverter/defibrillators. In particular, the invention relates to a system and method for transmitting telemetry data from such devices.").

As Per Claim 59: Claim 59 is substantially a restatement of claim 1 and is rejected under substantially the same reasoning. An apparatus performing the indicated function inherently has a means for doing so.

As Per Claim 61: The rejection of claim 60 is incorporated and further Arx et al. teaches:

- the implantable medical device maintains patient health information in an encrypted form

(Arx et al., Paragraph [0012], "Encryption refers to cryptographic algorithms which are used to encode messages in such a way that they cannot be read without possession of a special key that decrypts the message. Encryption of a message is performed by applying an encryption function to the message, where the encryption function is defined by a cryptographic algorithm and an encryption key. In the following

descriptions and referenced drawings, such an encrypted message will be designated as E(m,k), where E is the encryption function, m is an unencrypted message, and k is the key used to encrypt the message. Decryption of a message involves the application of a reverse function D to an encrypted message m using a decryption key k, designated as D(m,k).").

As per Claim 65: The rejection of claim 60 is incorporated and further Arx et al. teaches:

- the implantable medical device maintains patient health information in an unencrypted form and is accessible in the unencrypted form exclusively through a short range telemetric connection

(Arx et al., Paragraph [0023], Lines 15-19 "In a second embodiment limited information is allowed, but programming of the device is not. This embodiment supports remote patient monitoring without the patient having to release the interlock.").

As Per Claim 68: The rejection of claim 60 is incorporated and further Arx et al. teaches:

- the long range interface is augmented using one or more repeaters

(Arx et al., Paragraph [0031], Lines 28-33 "In the case where long-range telemetry is implemented over a network, the receiver/transmitter pair of external device

2 would be interfaced to a network connection, while the implantable device would 1 would be wirelessly interfaced to a repeater unit with a network connection.").

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin A Kaplan/
Examiner, Art Unit 2434

/Michael J Simitoski/
Primary Examiner, Art Unit 2439